Akamai Customer Story

Financial Firm Discovers and Secures APIs

A bank protected its digital initiatives by uncovering hidden APIs, assessing and mitigating API risk, and meeting regulatory demands

Gained full visibility | Improved security posture | Secured digital initiatives

The financial services industry is rapidly embracing digital transformation to stay competitive in an ever-evolving market. By using digital capabilities like artificial intelligence and big data analytics, financial institutions are able to offer innovative products, reduce costs, and provide more personalized and efficient services to their customers.

At the same time, digital transformation brings with it an increased risk of cyberattacks. To combat this growing issue, cybersecurity is now an essential part of any digital transformation strategy. Financial services firms must ensure that their systems are secure and resilient to protect their customers' data and assets from malicious actors.

One of Asia's prominent commercial banks quickly sought out Noname Security (now an Akamai company) to help fortify their API security posture. API breaches have reached alarming rates; Tech Wire Asia pointed out that "today, as many as 1 in every 13 cyber incidents can be attributed to API insecurity." They also stress that "API vulnerabilities cost businesses up to US$75 billion annually."

Considering our customer has more than US$700 billion in total assets, 5,000+ corporate customers, and a world-renowned wealth management reputation, it was imperative that all API vulnerabilities be addressed as soon as possible.

Financial Services

Location

Asia

Industry

Financial Services

Solution

Akamai API Security

A need for greater visibility into APIs and their risks

The institution had already deployed an API management platform for authentication and traffic control, but there were doubts about its ability to prevent API abuse and cyberattacks. Though API gateways provide much-needed, basic API security controls, they are unfortunately not enough to adequately protect organizations from API-specific threats.

For example, Broken Object Level Authorization, often referred to as BOLA, appears as normal API traffic to gateways. This lack of contextual awareness between API requests and responses enables BOLA attacks to pass through undetected and access critical back-end services. Not only can this flaw leave the organizations vulnerable to BOLA exploits, it can also open the door to other attacks and business logic abuse.

Another visibility limitation involves maintaining an accurate API inventory. As with most large organizations, the bank was struggling with unknown APIs in their environment. The reality is: Enterprises manage thousands of APIs, many of which are not routed through a proxy such as an API gateway. These are referred to as rogue APIs or zombie APIs. These APIs were likely deployed by former employees or before the organization got serious about API security. Regardless of the reason they exist, the bank's API gateway couldn't see them, so it became easy to underestimate just how many APIs they had.

Rising to meet the API security challenge

The organization deployed the complete Noname API Security Platform (now part of Akamai API Security), including solutions for API posture management, runtime protection, and testing across their environment. The customer's security posture improved exponentially as they are now able to detect and remediate vulnerabilities for one the world's most obscure threat vectors.

Now unknown APIs can be discovered and revealed within the platform, enabling complete visibility and risk mitigation. The institution has dramatically reduced its API sprawl and improved compliance, as Akamai API Security classifies sensitive data to help satisfy regulations like GDPR, HIPAA, and more.

The bank also now has the ability to stop attacks in real time and protect customer data assets. The runtime protection solution intelligently detects and prioritizes potential threats while continuously monitoring API activity. By integrating with web application firewalls, API gateways, security information and event management, information technology service management, and other workflow tools, our platform enables threat remediation manually, partially automatically, or automatically.

Results

APIs have quickly become a preferred attack vector for hackers, and the attacks show no signs of slowing down. For example, we saw "a 257 percent growth in the number of attacks against financial services year over year" in 2022. The financial services firm will be well-equipped to avoid becoming a statistic and to defend against this trend thanks to Akamai API Security. In particular, the customers' security teams will have a better understanding of the dangers that APIs present and be able to create systems that are even more secure.

| Support | | Published 08/24